Network Security

**Key Terms for Domain 4 - Network Security:**

1. **OSI Model**:
   * Layer 1: Physical Layer
   * Layer 2: Data Link Layer
   * Layer 3: Network Layer
   * Layer 4: Transport Layer
   * Layer 5: Session Layer
   * Layer 6: Presentation Layer
   * Layer 7: Application Layer
2. **TCP/IP Model**:
   * Network Interface Layer
   * Internet Layer
   * Transport Layer
   * Application Layer
3. **Network Topologies**:
   * Star
   * Mesh
   * Bus
   * Ring
4. **IP Addressing**:
   * IPv4
   * IPv6
   * Subnetting
   * CIDR (Classless Inter-Domain Routing)
   * Private vs. Public IPs
   * Network Address Translation (NAT)
5. **Routing Protocols**:
   * Static vs. Dynamic Routing
   * Distance Vector (e.g., RIP)
   * Link State (e.g., OSPF)
   * Border Gateway Protocol (BGP)
6. **Transmission Protocols**:
   * TCP (Transmission Control Protocol)
   * UDP (User Datagram Protocol)
   * ICMP (Internet Control Message Protocol)
7. **Ports and Protocols**:
   * Well-Known Ports (0-1023)
   * Registered Ports (1024-49151)
   * Dynamic/Private Ports (49152-65535)
   * Common Protocols: HTTP, HTTPS, FTP, SSH, DNS, SMTP, POP3, IMAP
8. **Network Devices**:
   * Router
   * Switch
   * Hub
   * Firewall
   * Gateway
   * Load Balancer
   * Proxy Server
9. **Virtual Private Network (VPN)**:
   * Site-to-Site VPN
   * Remote Access VPN
   * SSL/TLS VPN
   * IPSec VPN
10. **Firewall Types**:
    * Packet Filtering Firewall
    * Stateful Inspection Firewall
    * Proxy Firewall
    * Next-Generation Firewall (NGFW)
11. **Intrusion Detection/Prevention Systems (IDS/IPS)**:
    * Signature-based Detection
    * Anomaly-based Detection
    * Host-based IDS (HIDS)
    * Network-based IDS (NIDS)
12. **Network Segmentation**:
    * VLANs (Virtual Local Area Networks)
    * DMZ (Demilitarized Zone)
    * Microsegmentation
13. **Network Security Threats**:
    * DDoS (Distributed Denial-of-Service) Attacks
    * Man-in-the-Middle Attacks (MITM)
    * IP Spoofing
    * Phishing
    * SQL Injection
    * ARP Spoofing
14. **Network Security Controls**:
    * Firewalls
    * Intrusion Detection/Prevention
    * Network Access Control (NAC)
    * Security Information and Event Management (SIEM)
    * Honeypots
15. **Wireless Networking**:
    * Wi-Fi Standards (802.11 a/b/g/n/ac/ax)
    * WPA, WPA2, WPA3
    * WEP (Wired Equivalent Privacy) – deprecated
    * Wireless Access Points (WAP)
    * SSID (Service Set Identifier)
    * Wireless Security (PSK, 802.1X, EAP)
16. **Encryption and VPN Security**:
    * TLS (Transport Layer Security)
    * SSL (Secure Sockets Layer)
    * IPSec (Internet Protocol Security)
    * Encryption Algorithms (AES, RSA)
    * Public Key Infrastructure (PKI)
17. **Network Monitoring Tools**:
    * SNMP (Simple Network Management Protocol)
    * NetFlow
    * Wireshark
    * Nmap
18. **Zero Trust Architecture (ZTA)**:
    * Principle of least privilege
    * Continuous authentication and verification
19. **Network Policies**:
    * Acceptable Use Policies (AUP)
    * Security Policies
    * Network Baseline
20. **Cloud Networking**:
    * Software-Defined Networking (SDN)
    * Virtual Network Functions (VNF)
    * Public, Private, Hybrid Cloud

The **OSI (Open Systems Interconnection) Model** is a conceptual framework used to understand and standardize the functions of a networking system. It divides communication into **7 layers**, where each layer performs a specific role in the process of transmitting data from one device to another. Let me explain each layer with a **real-world example** to demonstrate how the model works in practice.

**1. Physical Layer (Layer 1):**

This is the **hardware** layer. It deals with the actual physical connection between devices, such as cables, switches, and electrical signals. It transmits raw binary data (0s and 1s) over the physical medium.

**Example:**

Imagine sending a **letter** by post. The physical layer is like the **postal truck** that physically carries your letter from your home to the destination. It doesn't care what the letter contains; its job is just to deliver the physical item (envelope).

**2. Data Link Layer (Layer 2):**

This layer ensures **error-free** transmission between two devices directly connected to the same network, like devices in a local area network (LAN). It organizes the data into frames and handles **MAC addresses** (Media Access Control).

**Example:**

In the letter analogy, this is the **address written on the envelope**. The postal worker uses the address to make sure the letter is delivered to the correct house in the local area.

**3. Network Layer (Layer 3):**

This layer is responsible for **routing** the data between different networks, like the Internet. It handles **IP addresses** and determines the best path for the data to travel to reach its destination.

**Example:**

The **postal system** between different cities. If you're sending a letter from Toronto to New York, the network layer ensures that the postal service finds the best route for the letter to travel from one city to another.

**4. Transport Layer (Layer 4):**

This layer manages **end-to-end communication** and ensures reliable data transfer. It breaks down the data into segments, manages flow control, and ensures error recovery. Key protocols here are **TCP** (Transmission Control Protocol) and **UDP** (User Datagram Protocol).

**Example:**

Imagine you've written a **long letter**, but the postal system only allows you to send a few pages at a time. The transport layer is like sending the letter in multiple **envelopes** and making sure the receiver can put the pages back together in the correct order. If any envelope goes missing, the sender is notified, and a resend can happen.

**5. Session Layer (Layer 5):**

This layer controls the **dialogue** between two devices. It establishes, manages, and terminates communication sessions between applications.

**Example:**

When you start a **phone call**, the session layer is responsible for establishing the connection between you and the other person. Once you're done, the session layer helps to properly **end** the call. It manages the start, ongoing communication, and closure of the session.

**6. Presentation Layer (Layer 6):**

This layer translates data between the application layer and the network. It handles **data encoding, encryption, and compression**, ensuring that data is in the correct format for the application to read.

**Example:**

If you are sending a **message in code** (like secret letters with encryption), the presentation layer ensures that the message is **encoded** at the sender's end and **decoded** at the recipient's end. For example, if you send the message in French and the recipient understands only English, this layer translates the content so both parties can understand.

**7. Application Layer (Layer 7):**

This is the topmost layer, where the **user interacts directly** with the network through applications like web browsers, email clients, and file transfer programs. It facilitates network services for the end-user.

**Example:**

Opening **Gmail** to send an email is an application layer interaction. The application layer provides the interface to send or receive the data (in this case, the email). It’s like sitting down and writing the actual **letter** using a pen and paper. This is the user’s direct interaction with the process.

**Complete Real-Life Example:**

Suppose you’re sending an email with a large attachment from your computer in Toronto to a friend's computer in New York:

1. **Physical Layer**: Your computer’s network card converts the data into electrical signals or wireless signals that pass through your home router.
2. **Data Link Layer**: The router assigns the MAC address of your computer and sends the data to your ISP (Internet Service Provider).
3. **Network Layer**: The data is assigned an IP address and routed through the internet, across different networks, to reach your friend's ISP in New York.
4. **Transport Layer**: Your email (which may be large) is split into smaller data packets. If any packet gets lost during transmission, this layer ensures it gets retransmitted.
5. **Session Layer**: A communication session is established between your email server (in Toronto) and your friend's email server (in New York).
6. **Presentation Layer**: The email attachment (perhaps a compressed file) is decoded and decompressed at your friend's end so they can view it properly.
7. **Application Layer**: Your friend opens their email client (like Gmail) and reads the email and attachment you sent.

Each of these layers works together to ensure that the data (your email) is successfully transmitted and understood by both you and the recipient, even though it's traveling across vast distances and through many different networks.

4o